NOTICE

U S DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

N 1370.37

Cancellation
Date: June 7, 2003

SUBJ: INTERNET ACCESS POINT CONFIGURATION MANAGEMENT

1. **PURPOSE.** This notice prescribes minimum configuration requirements for all recognized FAA Internet Access Points (IAPs).

2. **DISTRIBUTION.** This document is distributed to the division level in Washington headquarters, regions, and centers and a limited distribution to all field offices and facilities.

3. **SCOPE.** This document applies to the IAPs designated in FAA Order 1370 83, Internet Access Points.

4. **BACKGROUND.** FAA Order 1370.82, Information Systems Security Program (ISSP), states that the Office of the Assistant Administrator for Information Services and Chief Information Officer (AIO-1) is authorized to issue detailed information systems security (ISS) implementation orders, procedures, and guidance. The FAA currently provides Internet access to its employees and on-site contractors through arrangements with commercial Internet service providers (ISPs) through recognized IAPs authorized by Order 1370.83. This notice serves as an implementation directive to Order 1370 83.

5. **ACTION.** Each IAP administrator is required to implement the components defined in Figure 1, Required IAP Configuration, and described in paragraph 7 below within 90 days of the approval date of this notice.

6. **DEFINITIONS.** Appendix 1, Definitions, contains terms used in this notice

7. **PROCEDURE.** Each IAP shall implement the equipment and management procedures outlined in paragraphs 7a and 7b below:

a. Required Protection.

(1) Perimeter Router. IAP sites are required to install and manage a local, FAA-controlled, external (frontwall) router at each IAP within 90 days of the approval date of this notice. All other routers (e.g., backwall routers) connected directly to an ISP are unauthorized. Only FAA personnel or FAA on-site contractors will manage perimeter routers. Routers will be configured in accordance with the FAA Router Configuration Guide when released by AIO no later than August 30, 2002.

(2) Switches. A 10/100 Ethernet switch will be installed between the perimeter router and the redundant firewalls. A second switch will be installed between the redundant firewalls and the backwall router. These switches will be used to connect the Intrusion Detection System (IDS) devices and the Internet monitoring capability (IMC), as well as network and traffic analyzers. The switches must have the ability to accomplish the following actions:

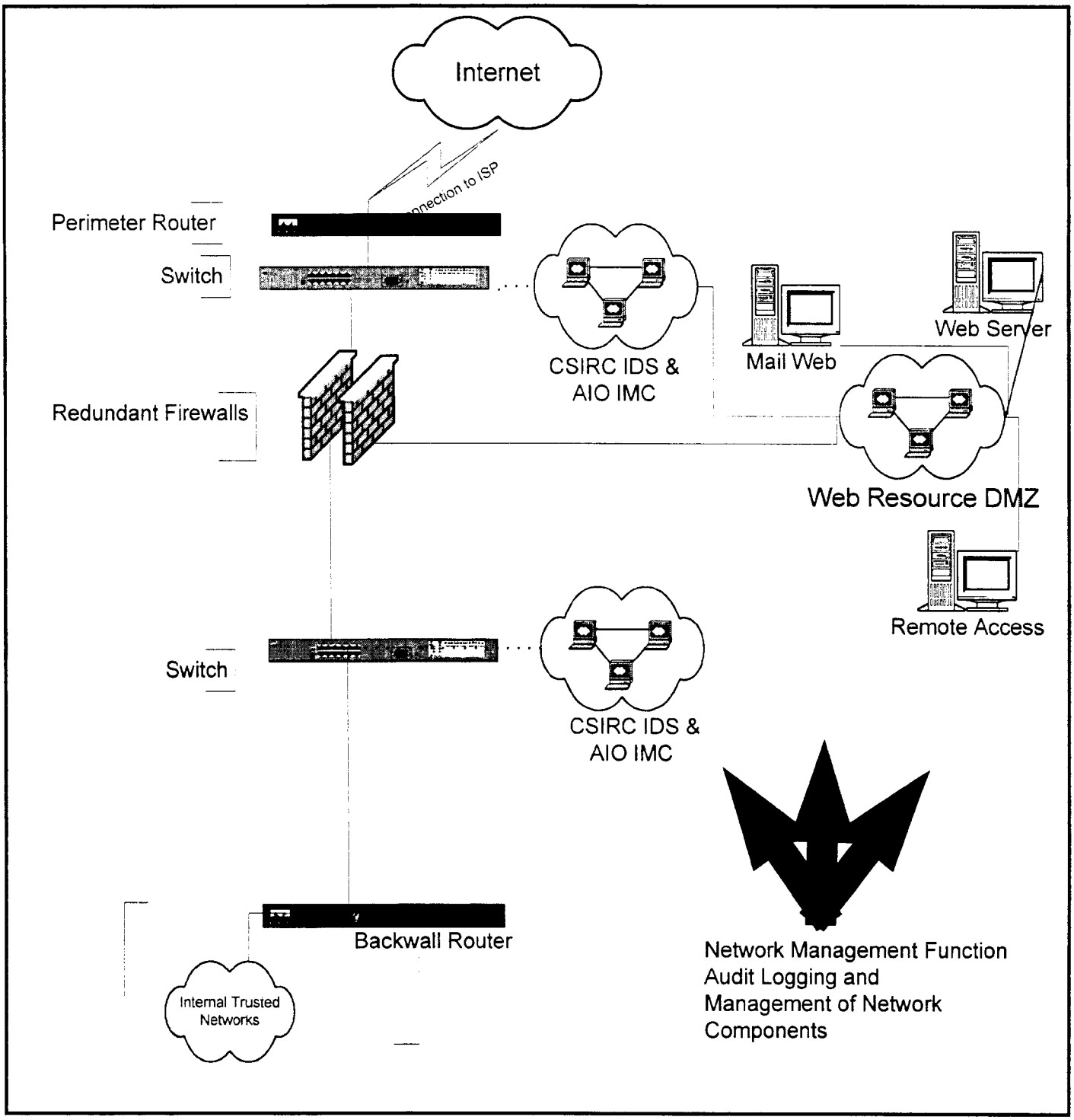

Figure 1 - Required IAP Configuration

(a) lock each port to prevent unauthorized physical access

(b) restrict a port to a particular Internet Protocol or media access control address

(c) create multiple span ports to direct all network traffic to a specific port

(d) restrict administrative access to the device

(e) block transmission of data from a given port while in span mode

(3) Redundant Firewalls. IAP sites are required to have redundant firewalls to support multiple interfaces with a minimum of one to the external, one to the internal, and one to the demilitarized zone(s) (DMZ). Basic filtering controls for incoming connections to this device are configured in accordance with the FAA Firewall Configuration Guide when released by AIO no later than September 30, 2002. Outbound filtering controls are implemented and outlined in the FAA Firewall Configuration Guide.

(4) Demilitarized Zone (DMZ). IAPs are required to establish a dedicated DMZ for all resources made available to the public. DMZ resources must be connected to each of the redundant firewall interfaces. DMZ devices are prohibited from initiating connections anywhere, unless explicitly permitted by the IAP administrator. Any site requiring multiple DMZs, at a minimum, is required to establish the same level of security for each DMZ or DMZ segment as described in this notice. Creation of an extended DMZ within an IAP is acceptable provided each connection into the extended DMZ is configured in accordance with this notice. For configuration purposes, the FAA considers any DMZ to be a hostile network to the internal FAA networks. Routing within the DMZ is permitted.

(5) Intrusion Detection System (IDS). IDS sensors installed at all IAPs will be non-intrusively managed, monitored, and maintained by the Computer Security Incident Response Center (CSIRC). IDS sensors will be placed in front of and behind the redundant firewalls. Additional IDS sensors are permitted.

(6) Internet Monitoring Capability (IMC). All IAPs shall have two Internet monitoring devices installed and monitored by AIO. One device will reside in front of the redundant firewalls to monitor incoming Internet traffic, and one device will reside inside the redundant firewalls to monitor outgoing Internet traffic.

(7) Network Management. All IAP devices are administered out-of-band or using a secure transport protocol such as secure shell or secure sockets layer.

(8) Virus Filter. All IAP sites shall have a virus filter in the DMZ to search incoming hypertext transport protocol, file transfer protocol (FTP), and simple mail transfer protocol for binary signatures (patterns) of known viruses.

b. Optional IAP Enhancements.

(1) Virtual Private Networks (VPNs). VPNs use advanced encryption and tunneling to permit organizations to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or extranets. Users who implement VPNs will be required to follow the VPN Configuration Guide when released by AIO no later than January 30, 2003. There are three types of VPNs. Each type requires written rules of behavior or a memorandum of understanding between the parties.

(a) Dedicated point-to-point tunnels. High-speed broadband connections that provide a cost-effective solution for connecting remote offices and extranets.

(b) User-to-Enterprise for Telecommuters. VPNs that allow mobile workers, telecommuters, and FAA authorized users to gain access to the FAA intranet, providing users significant flexibility and efficiency.

(c) Internal users to external enterprises. IAPs that allow FAA personnel to access external enterprises in support of an FAA business need.

(2) Cache Engines. Referred to as content delivery devices, these are devices close to users that save (cache) Web pages and possibly FTP and other files that all server users have requested so that successive requests for these pages or files can be satisfied by the cache server rather than requiring the use of the Internet. A cache server not only serves its users by getting information more quickly but also reduces Internet traffic. Cache engines are essential for enhancing performance in saturated networks and accelerate content delivery. A cache server is almost always also a proxy server.

(3) Proxy Servers. Proxy servers represent users by intercepting their Internet requests and managing them. Proxy servers are required because ADTN 2000 does not enable default routing. A proxy server helps match incoming messages with outgoing requests and is in a position to also cache the files that are received for later recall by any user. To the user, the proxy and cache servers are invisible; all Internet requests and returned responses appear to be coming from the addressed place on the Internet.

8. IAP PHYSICAL SECURITY. All IAP equipment is subject to FAA regulations for physical security in accordance with FAA Order 1600.69, FAA Facility Security Management Program. Physical access to routers, firewalls, and switches must be tightly controlled to preclude any unauthorized changes to the firewall configuration or operational status and to eliminate any potential for unauthorized monitoring of firewall or router activity.

9. ROLES AND RESPONSIBILITIES. FAA personnel have the following roles and responsibilities, consistent with those defined in FAA Order 1370.83. This paragraph contains additional roles and responsibilities.

a. Office of Information Services and Chief Information Officer (AIO).

(1) Office of the Assistant Administrator for Information Services and Chief Information Officer (AIO), installs and manages IMC devices.

(2) Office of the Director of Information Systems Security (AIS):

(a) Provides ISS policy and guidance to IAPs through the Configuration Control Committee, and ISS managers (ISSMs).

(b) Monitors and ensures compliance with this FAA notice.

(c) Provides resources to IAP sponsors to purchase necessary items to meet the security requirements of this notice.

(d) Coordinates with IAP administrator to verify effectiveness of security configuration(s).

(e) Provides filtering recommendations to be utilized at the perimeter routers so that traffic is filtered before getting to the internal FAA network.

b. The IAP Sponsoring Organization.

(1) Purchases necessary items to meet the above security requirements with funding provided by AIS.

(2) Assigns responsibilities to and manages IAP administrators.

(3) Ensures all IAP administrator positions have been designated high risk and the background investigations have been completed prior to appointed personnel occupying these positions in accordance with FAA Order 1600.1D, Personnel Security Program.

(4) Ensures that IAP administrators have a sound understanding of network concepts and implementation; knowledge of transmission control and Internet protocols; hands-on experience with networking concepts, design, and implementation so that IAP equipment is configured correctly and administered properly.

(5) Ensures IAP administrators receive regular training on the firewall(s) in use and on network security principals and practices to ensure currency.

(6) Ensures overall system responsibility resides within the FAA and that only FAA employees are assigned to the role of IAP administrator (in charge of the operations and maintenance of the IAP).

(7) Ensures at least two IAP administrators (one primary and alternate(s)) are designated by the IAP sponsor to be responsible for the upkeep of all IAP equipment.

(8) Ensures twenty-four by seven availability of IAP administrator to respond to outages or security events and that the CSIRC has pertinent information necessary to contact said administrator.

(9) Ensures major changes to all IAP components (except firewalls) are approved through a sponsoring organization's configuration management control board before implementation. Firewall changes are addressed in the FAA Firewall Configuration Guide.

(10) Establishes and maintains controls for disaster recovery and availability of personnel in the event of an outage or incident according to continuity of operations and contingency planning guidelines described in FAA Orders 1370.82 and 1370.83.

(11) Ensures systems are in compliance with the guidelines in their system certification and authorization plans.

(12) Provides contact information to AIS-1 and the CSIRC.

c. Internet Access Point Administrator.

(1) Maintains an extremely high level of knowledge about the configuration of the IAP system, inherent security weaknesses in the use of the system components, and FAA security policy.

(2) Creates secure IAP administrative controls and establishes access privileges, session controls, timeout controls, and software and account management controls in concert with the ISSM.

(3) Ensures new firewalls, virus filters, and routers are installed according to the guidelines of this notice.

(4) Implements and maintains the security controls defined in this notice for all equipment under IAP management.

(5) Maintains current inventory and point of contact information for all equipment and interfaces located within the IAP, including systems hosted in the DMZ.

d. The Information Systems Security Manager. Conveys security information to the IAP administrator and ensures necessary actions are taken to mitigate risk.

Arthur Pyster

for Daniel J. Mehan
Assistant Administrator for Information Services
and Chief Information Officer

APPENDIX 1. DEFINITIONS

Computer Security Incident Response Center (CSIRC). The FAA's 24/7 computer center. The CSIRC monitors FAA network activity and outages, processes all reports of computer security incidents against FAA IAPs; installs, operates, and maintains intrusion detection systems (IDSs) at the IAPs; and provides the local IAP administrators with access to IDS data relative to their IAP.

Configuration Control Committee (CCC). A committee designed to provide guidance for all issues relating to IAP configuration management and access to FAA systems and resources, perform comprehensive reviews of IAP justification papers, and review requests for deviation from IAP standards. This committee also makes recommendations on network, hardware, and software requirements, equipment standards; component configurations; and protocols and services authorized at each IAP.

Demilitarized Zone (DMZ). A computer host or small network inserted as a "neutral zone" between an organization's private network and the outside public network. In practice, DMZs act as proxy servers to prevent outside users from getting direct access to a server containing proprietary data, while supplying publicly available information.

Internet Access Point (IAP). Any physical or logical connection to the public Internet. An IAP includes any direct or permanent connection or any dial-up or temporary connection to the Internet.

IAP Administrator. An individual responsible for the configuration, account management, and performance of a computer network.

Internet Access. The connection to the public Internet or access to any Internet resource or information using any application, program, software, utility, or tool, for any reason or duration. For the purpose of this document, Internet access includes any permanent or temporary connection to the Internet.

Internet Monitoring Capability (IMC). A proprietary program, located on a proxy server at a network gateway, that monitors and logs all Internet events, either going toward an ISP router or coming from an ISP router, to monitor usage.

Internet Service Provider (ISP). The connection point or organization outside the FAA, connected either physically or logically to an IAP, that is the means by which the IAP gains access to the Internet.

Internet. A global network of independent hosts and communications facilities that connect users to those hosts. The term "Internet" also may refer to the content presented on the hosts or transmitted through the network. The FAA may contribute information and resources to the Internet for public consumption.

Intranet. The FAA's internal or private network used to share information and resources within the FAA community. Information and resources on the Intranet are not made available to the public.

Intrusion Detection System (IDS). A type of security management system for computers and networks that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

Network. Communications hardware and software that allow one user or system to connect to another user or system and can be part of a system or a separate system. Examples include local area networks, wide area networks, and public networks such as the Internet.

Perimeter Router. A device that routes data between one or more networks and a third-party Internet gateway. A perimeter router is sometimes contrasted with a core router, which forwards packets to computer hosts within a network (but not between networks). A perimeter router is an example of an edge device and is sometimes referred to as a boundary router.

Redundant Firewalls. A set of related programs, located at a network gateway server, protecting the resources of a private network from users from other networks. A firewall examines each network packet to determine whether to forward it toward its destination. The firewall allows remote access in to the private network or DMZ by the use of secure logon procedures and authentication certificates. Redundant firewalls allow all of the above measures to happen by working in series. If one firewall fails, the redundant firewall next in the series will take over the functionality. Redundant firewalls provide a measure of security so that there is no single point of failure.